Hastings Law Journal

Volume 60 | Issue 5 Article 6

1-2009

Passwords and Keys under the DMCA: A Call for Clarification from the Courts or Congress

Lindsey M. Shinn

Passwords and Keys Under the DMCA: A Call for Clarification from the Courts or Congress

LINDSEY M. SHINN*

INTRODUCTION: THE DIGITAL MILLENNIUM COPYRIGHT ACT

Congress passed the Digital Millennium Copyright Act ("DMCA" or the "Act") in 1998 to prevent the piracy of copyrighted works and to provide copyright owners with an incentive to develop new business models that would make these works available in digital form.[1] The DMCA provides copyright holders with three causes of action surrounding the circumvention of two types of "technological protection measures" (TPMs) that guard their works: the Act prohibits (i) the circumvention of "access" controls, and (ii) the trafficking in devices that are primarily designed to circumvent access or "rights" controls (measures that protect the specific bundle of rights encompassed by copyright).[2] Congress' purported purpose was to maintain the balance of

---

* J.D. Candidate, University of California, Hastings College of the Law, 2009. The Author would like to thank Professor Margreth Barrett, Lonnie, and Corbett for their comments on her drafts, the Volume 60 staff of the *Hastings Law Journal* for their careful eyes and expert corrections, and Roxane, Max, and Samir for their support.

1. *See* Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1135 (2003); Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law*, 50 J. COPYR. SOC'Y 113, 124 (2003).

2. First, "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A) (2006). Second:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title[.]

Id. § 1201(a)(2)(A)–(B). Third, and finally:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright

copyright, between protecting artists' works and encouraging further creativity, as we advance into the digital age. Commentators have since debated whether that goal has actually been achieved. Some believe the DMCA is beneficial and necessary to spur the availability of copyrighted works in digital formats and on the Internet.[3] Critics of the DMCA, however, argue the statute actually upset the balance of copyright, tilting it unfairly in favor of copyright owners.[4]

Though the legislative history of the Act mentions the Internet and content media as key concerns in the battle against piracy,[5] whether or not Congress intended it, once implemented, the DMCA proved to be relevant in a whole host of other areas. For example, the broadest question arising in the context of section 1201(a)(1) is whether Congress intended to prohibit circumvention of TPMs only when it then leads to the possibility of copyright violation,[6] or whether it created a new right of "access" separate and apart from the Copyright Act itself.[7] In the case of electronics parts embedded with copyrightable computer code, courts such as the Federal Circuit in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, and the Sixth Circuit in *Lexmark International, Inc. v. Static Control Components, Inc.*, recognize that Congress did not intend for the DMCA to affect the aftermarket for spare parts.[8] These courts have agreed that with respect to products such as garage door openers and printers, plaintiffs should not be able to obtain a monopoly on secondary parts simply because they are partially comprised of electronics that communicate with each other through "handshake" methods that merely resemble TPMs.[9]

Courts have been fairly clear about where and how they believe the DMCA applies. However, these decisions often seem outcome

---

owner under this title in a work or a portion thereof; [or]

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof[.]

Id. § 1201(b)(A)–(B).

3. Jane C. Ginsburg, *Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the U.S. Experience*, 29 COLUM. J.L. & ARTS 11, 26 (2005).

4. *See, e.g.*, R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619 (2003); Jerome H. Reichman et al., *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981 (2007); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

5. 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.02(A) (2008).

6. *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1182 (Fed. Cir. 2004).

7. Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001); Ginsburg, *supra* note 1. However, this question is beyond the scope of this Note.

8. *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004); *Chamberlain*, 381 F.3d at 1178.

9. *Lexmark*, 387 F.3d at 530; *Chamberlain*, 381 F.3d at 1199–1201.

determinative in the closer cases, based upon who is doing the circumventing and for what purpose. For example, when the use of a device is clearly directed toward accessing or copying unpaid-for copyrighted works, such as movies and musical recordings, courts tend to hold that the device circumvents in violation of sections 1201(a)(2) and 1201(b)(1).[10] Conversely, *Lexmark* and *Chamberlain* held that the DMCA did not apply in the aftermarket-parts context.[11] However, some of the cases that are less obviously circumvention often skip crucial parts of the analysis in explaining exactly how and why the conduct at issue offends the circumvention provisions of section 1201.[12] This Note contends that many of these decisions make serious logical reasoning errors in attributing DMCA liability to defendant conduct when compared to the text of the statute. This has led to inconsistency across the broad spectrum of DMCA decisions.

This Note specifically addresses the courts' treatment of the DMCA in the gray area of "passwords" or "keys" in the narrow class of cases that I will refer to as "password" cases. Here, courts and commentators often split over when the application of a legitimate, copyright-holder–issued password or key to a TPM constitutes impermissible circumvention under section 1201.[13] This issue raises a whole host of questions. When, if ever, does the use of a password constitute "circumvention" under the statute? Does this use hinge on the "authority" of the copyright holder? How does one know when such authority exists? What if a valid password is obtained and applied by someone who is not explicitly "authorized"? Can a more technologically sophisticated software code "key" ever constitute a permissible "password" under the statute?

In discussing passwords and keys used to move past TPMs, this Note is primarily concerned with the definition and application of the phrase to "circumvent a technological measure."[14] Under section 1201(a)(3)(A), it means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[15] In section 1201(b)(2)(A), the definition of circumvention is slightly

10. *See infra* Parts I, III.

11. *See infra* Part II.

12. *See, e.g.*, Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1184 (E.D. Mo. 2004); 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004); *see also* discussion *infra* Part III.

13. *See, e.g.*, Ginsburg, *supra* note 3, at 27–28 ("This interpretation is questionable. . . . Entry of the password 'deactivates' the measure that restricts access; if the password is employed by an unauthorized user, then the deactivation will not have occurred with the copyright owner's authority." (citations omitted)). However, this is a very subjective definition of authorized.

14. *See* 17 U.S.C. § 1201(a)(3)(A), (b)(2)(A) (2006).

15. *Id.* § 1201(a)(3)(A).

different: "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."[16] It is important that the latter says nothing about the "authority of the copyright owner," and the former does not define authority at all.

The first Part of this Note will address the clearer types of cases covered by the DMCA—the hacking and intent to circumvent cases on one side and the replacement electronics parts cases on the other. Next, the discussion will delve into the password cases, which constitute a gray area of uses that are not obviously circumvention, but are often held to be. Described the right way, many more "applications of information" to TPMs can constitution proper "access" than the courts currently allow or that Congress may have intended.[17] However, failure to acknowledge this ambiguity leaves us with an illogical and inconsistent interpretation of the circumvention provisions of the DMCA.

The final Part of this Note suggests that Congress or the courts should better define the definition of "circumvention" and what constitutes "authority" under section 1201. This process becomes challenging when considering the differing infrastructures upon which the DMCA sits. The current world of the First Sale Doctrine gives one with title to a legal copy of a copyrighted work the right to do what one wishes with it.[18] However, some argue Congress endorsed the evolving trend of "renting" works to consumers through pay-per-use licensing agreements, which are designed to make works more freely and cheaply available.[19] Under this scheme, the First Sale Doctrine does not apply. With these two models in mind, should the fact that one owns or possesses the work constitute authority of the copyright owner? Yes, under the first model, but not under the second; for if you possess the work but only purchased a limited-use version, you only have limited "authorization" to access it. Society is likely at a place between these two models, and therefore the DMCA and its current definitions are an uncomfortable fit. Congress should reevaluate its one-size-fits-all model.

16. *Id.* § 1201(b)(2)(A).

17. *Id.* § 1201(a)(3)(B).

18. *Id.* § 109 ("[T]he owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord."); Pamela Samuelson, *The Copyright Grab*, WIRED MAG., Jan. 1996, *available at* http://www.wired.com/wired/archive/4.01/white.paper_pr.html.

19. *See, e.g.*, Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium,"* 23 COLUM.-VLA J.L. & ARTS 137, 142 (1999).

I. BACKGROUND: CASES THE DMCA WAS INTENDED TO ADDRESS

With the advent of Napster and other online file sharing sites, it became easy for consumers to obtain copies of copyrighted work for "free."[20] In response, copyright owners began putting technological "locks" on their works. The DMCA was intended to be another tool to prevent copyright infringement in the digital environment, or more simply put, "piracy."[21] One of the ways it does this is to make it a violation to "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" that enables someone to circumvent a technological measure that protects access to a copyrighted work or a right of copyright.[22] The idea is that a ban on providing circumvention devices reduces their availability on the market, thus making it more difficult to gain unauthorized (i.e., unpaid) access to, and to infringe upon, copyrighted works.[23]

One of the most notorious areas of litigation under the DMCA involves the DVD-content-protection program known as the Content Scrambling System (CSS). A Norwegian programmer discovered a way around it, calling his circumvention mechanism "DeCSS."[24] Litigation ensued over the use of DeCSS, and whether the defendant's actions in making it available encouraged copyright infringement. For example, the court in *Universal City Studios, Inc. v. Reimerdes* found that DeCSS circumvented CSS under the meaning of the circumvention provisions of the DMCA.[25] Defendants were found liable for trafficking because, by their own admission, they posted DeCSS on their website, and its only function was to circumvent CSS.[26]

The court further noted that "the availability of DeCSS on the Internet effectively has compromised plaintiffs' system of copyright protection for DVDs, requiring them either to tolerate increased piracy or to expend resources to develop and implement a replacement system unless the availability of DeCSS is terminated."[27] The court analogized to

20. *See* Aaron M. Bailey, Comment, *A Nation of Felons?: Napster, the Net Act, and the Criminal Prosecution of File-Sharing*, 50 AM. U. L. REV. 473, 478–81 (2000).

21. Burk, *supra* note 1.

22. 17 U.S.C. § 1201(a)(2), (b)(1).

23. Burk, *supra* note 1, at 1135–36 ("The record suggests that the anticircumvention right was intended by Congress as a shield rather than as a sword, intended as a means to prevent wholesale misappropriation of copyrighted content, rather than as a means to extend content owners' exclusivity to cover adjacent, uncopyrighted technologies.").

24. *Id.* at 1112; *see also* Andy Patrizio, *Why the DVD Hack Was a Cinch*, WIRED MAG., Nov. 2, 1999, *available at* http://www.wired.com/science/discoveries/news/1999/11/32263.

25. 111 F. Supp. 2d 294, 318–19 (S.D.N.Y. 2000).

26. *Id.*

27. *Id.* at 315.

"the publication of a bank vault combination in a national newspaper. Even if no one uses the combination to open the vault, its mere publication has the effect of defeating the bank's security system, forcing the bank to reprogram the lock."[28]

On appeal to the Second Circuit as *Universal City Studios v. Corley*, the defendants argued, among other things, that "an individual who buys a DVD has the 'authority of the copyright owner' to view the DVD, and therefore is exempted from the DMCA pursuant to subsection 1201(a)(3)(A) when the buyer circumvents an encryption technology in order to view the DVD on a competing platform."[29] However, the court rejected this argument, noting that subsection 1201(a)(3)(A) "exempts from liability those who would 'decrypt' an encrypted DVD with the authority of a copyright owner, not those who would 'view' a DVD with the authority of a copyright owner," and that "Defendants offered no evidence that the Plaintiffs have either explicitly or implicitly authorized DVD buyers to circumvent encryption technology to support use on multiple platforms."[30] This decision laid the groundwork for how courts interpret the DMCA in the context of consumer media like CDs and DVDs. However, the court failed to fully explain the notion of "authorization" or how the defendants might have obtained it.

In the wake of *Corley*, another case arose that challenged the legality of a device accused of circumventing CSS. *321 Studios v. MGM Studios, Inc.* claims to be an offshoot of the prior case, in that it addresses the use of a program that could circumvent CSS, and basically follows the *Corley* analysis.[31] In *321 Studios*, plaintiff created a program called "DVD-X Copy" which could read the content of a DVD encoded with CSS and then copy it to a computer without the CSS encoding; this allowed the content to be played on any media, but also to be copied.[32] Essentially, the program used a CSS "player key" and "publicly known computer code" to decode CSS and access the data.[33] Although one was not supposed to be able to obtain a player key without entering into a license agreement, the opinion does not say how defendants obtained a copy.[34] The copyright holders here successfully framed the issue as one of authority under the CSS license agreement, as found by the court in *Reimerdes*:

---

28. *Id.*

29. 273 F.3d 429, 444 (2d Cir. 2001).

30. *Id.*

31. 307 F. Supp. 2d 1085 (N.D. Cal. 2004). This Note challenges some of the reasoning in this case. *See infra* Part IV.B.

32. 307 F. Supp. 2d at 1089.

33. *Id.*

34. *Id.*

> [O]nly licensed DVD players can legally access the CSS keys in order to play DVDs. *See Universal Studios v. Reimerdes*, 111 F.Supp.2d at 317–318 ("One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license.").[35]

The court agreed with this argument, finding circumvention and violation of the trafficking provisions in both section 1201(a)(2) and section 1201(b)(1) because, although the keys were valid, 321 Studios was not authorized to use them, and thus, their use constituted circumvention.[36]

II. UNINTENDED CONSEQUENCES: THE "AFTERMARKET-PARTS" CASES

Because computers are becoming increasingly ubiquitous in a variety of household products, and because computer programs are protected by copyright, litigation arose under the DMCA in the area of component parts that use "authentication keys" or electronic "handshakes" to communicate with the main product.[37] In the Federal Circuit cases of *Chamberlain* and *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, and in the Sixth Circuit decision in *Lexmark*, the plaintiffs sued parts makers under the DMCA, claiming that defendants' use of their keys constituted circumvention of their access and rights controls.[38] Both circuits, however, found no circumvention liability, and further rationalized that, in any case, the DMCA was not meant to reach this area.[39]

The Sixth Circuit noted in *Lexmark* that because plaintiff had not "directed any of its security efforts . . . to ensuring that its copyrighted work . . . cannot be read and copied," it could not claim to have put in place a "technological measure that effectively controls access to a work protected under [the copyright statute]."[40] Thus, the court highlighted the need for the technological measure at issue to actually protect the copyrighted work. Further, the *Chamberlain* court held that the DMCA "prohibits only forms of access that bear a reasonable relationship to the

35. *Id.* at 1095 (citation omitted) (quoting Universal Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000)).

36. *Id.* at 1099.

37. NIMMER & NIMMER, *supra* note 5, § 12A.06(C)(2).

38. Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1310 (Fed. Cir. 2005); Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 529 (6th Cir. 2004); Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1185 (Fed. Cir. 2004).

39. *Storage Tech.*, 421 F.3d at 1318; *Lexmark*, 387 F.3d at 549; *Chamberlain*, 381 F.3d at 1203–04. For a discussion of the DMCA legislative history generally, see *Chamberlain*, 381 F.3d at 1193–99.

40. 387 F.3d at 549 (citation omitted) (internal quotation marks omitted).

protections that the Copyright Act otherwise affords copyright owners."[41] Thus, to demonstrate a violation of section 1201(a), a copyright owner must prove that the alleged circumvention "infringes or facilitates infringing a right *protected* by the Copyright Act."[42] The Federal Circuit went even further in *Storage Technology*, disapproving of DMCA actions not directly connected to copyright infringement.[43]

Another important aspect these three cases explore is the issue of authorization. Professor Lipton noted that the *Chamberlain* court did not accept that defendant's conduct was unauthorized, and instead concluded that Chamberlain "implicitly authorize[d] its customers—to whom it distributes its software embedded in the remote control—to purchase any brand of transmitter that will open their garage door."[44] Similarly, the court in *Storage Technology* explored the concept of authorization, and the use of the DMCA to enforce contractual provisions. There, defendant was a repair company that fixed data storage libraries built by plaintiff.[45] To perform its work the company had to intercept maintenance error codes sent by plaintiff's data storage software embedded in the system.[46] To successfully intercept the codes, however, defendant's computers had to "override a password protection scheme," which defendant accomplished simply by having its software guess at the key until it found the right one.[47] Plaintiff argued this was foreclosed by the DMCA because it violated the initial sales contract.[48]

The *Storage Technology* court noted that "'uses' that violate a license agreement constitute copyright infringement only when those uses would infringe in the absence of any license agreement at all."[49] The plaintiff sold physical tape libraries but only licensed the necessary software.[50] That license covered only the "functional code portions of the software," which "specifically excludes the maintenance code. However . . . [b]oth the functional and maintenance code are automatically loaded into the RAM . . . upon startup, and copying the entire code is necessary to activate and run the library."[51] Storage Technology argued that even if its customers were authorized to access

41. 381 F.3d at 1202.

42. *Id.* at 1203 (emphasis added).

43. 421 F.3d at 1318 ("To the extent that [defendant's] activities do not constitute copyright infringement or facilitate copyright infringement, [plaintiff] is foreclosed from maintaining an action under the DMCA.").

44. Jacqueline Lipton, *The Law of Unintended Consequences: The Digital Millennium Act and Interoperability*, 62 WASH. & LEE L. REV. 487, 511 (2005).

45. *Storage Tech.*, 421 F.3d at 1310.

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.* at 1316.

50. *Id.* at 1310.

51. *Id.*

the maintenance codes, its customers could not in turn authorize defendants, because customers were not permitted to "sublicense, assign, lease or permit another person to use" the codes.[52] The court disagreed, noting that other portions of the license agreements demonstrated "the authorized use is tied to a particular machine, rather than a particular person."[53] This is not dissimilar from the notion that a legitimately issued password, even in the hands of someone other than to whom it was originally issued, may use it without committing circumvention under section 1201(a).

Proceeding to Storage Technology's DMCA claim, the court argued that even when circumvention is found under the DMCA, "[a] court must look at the threat that the unauthorized circumvention potentially poses in each case to determine if there is a connection between the circumvention and a right protected by the Copyright Act."[54] Noting the lack of copyright infringement here, and perhaps agreeing with defendant that "it [was] implicitly authorized to copy the maintenance code,"[55] the court held that "[t]he activation of the maintenance code may violate [Storage Technology's] contractual rights vis-à-vis its customers, but those rights are not the rights protected by copyright law. There is simply not a sufficient nexus between the rights protected by copyright law and the circumvention of the [plaintiff's] system."[56]

As one group of commentators recently noted, "[t]he courts ultimately decided these cases by permitting third-party suppliers of parts or services to bypass the lock-out codes and provide competing parts or services, notwithstanding . . . the DMCA. Judges in the lock-out cases could not accept the unbalanced interpretation of section 1201 . . . ."[57] However, other scholars argue that Congress did in fact intend 1201(a) to be a new right of access; that by granting it "without further requiring proof of a nexus between the circumvention and infringement, Congress has permitted, indeed encouraged, copyright

52. *Id.* at 1316 (internal quotation marks omitted).

53. *Id.* at 1316–17 ("[Storage Technology's] argument, however, ignores the rest of the license agreement. The prohibition on third-party use of the code is modified by a later provision stating that equipment owners 'may transfer possession of Internal Code only with the transfer of the Equipment on which its use is authorized.' Additionally, the license grants the customer the use of the code for 'the sole purpose of enabling the specific unit of Equipment for which the Internal Code was provided . . . .' The clear implication of those sections is that the license is tied to the piece of equipment on which the software resides. Thus, the authorized use is tied to a particular machine, rather than a particular person." (alteration in original)).

54. *Id.* at 1319.

55. *Id.* at 1311.

56. *Id.* at 1319.

57. Reichman et al., *supra* note 4, at 1011 (citation omitted).

owners to create and control markets for their works that the traditional exclusive rights under copyright would not secure."[58]

III. THE GRAY AREA: PASSWORDS VERSUS KEYS

This brings us to a gray area of DMCA law: the use of a password or key issued by the copyright holder, but in ways perhaps not contemplated or preferred by the copyright holder. These cases force courts to ask in a very specific way, what constitutes circumvention under the DMCA? The three issues this Part will discuss are: (1) when the use of a password or key is an act of circumvention, (2) when the user of a password or key of valid provenance uses it without the authority of the copyright owner, and (3) when the breach of a contract restriction triggers a DMCA violation. This area is where courts have been the least consistent in their interpretation of the DMCA, as these types of cases seem to be caught in the middle between the after-market parts cases like *Chamberlain* and the clear instances of hacking to circumvent access or copy controls as in *Corley*. This Note posits that one of the reasons is because neither Congress nor the courts have workably defined "authorization" within the definition of circumvention under the DMCA.

In the first case to address manually applied passwords under the DMCA, *I.M.S. Inquiry Management Systems. v. Berkshire Information Systems.*, the defendant allegedly "obtained a user identification and password issued to a third party" and "intentionally and without authorization accessed I.M.S.'s e-Basket service, and gathered and copied content therefrom."[59] After noting that the DMCA covers both "technologically-sophisticated" actions such as "decryption, descrambling, deactivation and impairment" and the more "open-ended and mundane" avoiding or bypassing, the court determined that defendant's actions did not fit any of these definitions.[60] Consequently, the court held that "[d]efendant did not surmount or puncture or evade any technological measure to [access the website]; instead, it used a password intentionally issued by plaintiff to another entity" and thus did not violate the DMCA.[61]

While some scholars and practitioners have criticized *I.M.S.*,[62] two courts have followed the decision. In *Egilman v. Keller & Heckman, LLP*, defendant law firm accessed plaintiff's password-protected website

58. Ginsburg, *supra* note 3, at 30.

59. 307 F. Supp. 2d 521, 523, 531 (S.D.N.Y. 2004) ("Whether accessing copyrighted work by unauthorized use of an otherwise legitimate, owner-issued password qualifies as circumvention . . . appears to be a question of first impression in this Circuit and in all others.").

60. *Id.* at 532.

61. *Id.* at 532–33.

62. *See, e.g.*, Ginsburg, *supra* note 3, at 27.

in the course of litigation between its client and the plaintiff.[63] However, rather than obtaining the username and password from a third party, the defendants may simply have guessed the correct one.[64] In dismissing Egilman's DMCA claim, the court stated that "*I.M.S.* was correctly decided" and "not factually distinguishable."[65] The court concluded that "using a username/password combination as intended—by entering a valid username and password, albeit without authorization—does not constitute circumvention under the DMCA."[66] In *Healthcare Advocates, Inc. v. Harding, Early, Follmer, & Frailey*, an even more recent case citing *I.M.S.*, the court noted that because there was essentially no technological protection measure to be circumvented, "lack of permission is not circumvention under the DMCA."[67]

All three courts characterized the actions of the defendants not as circumventing, but as properly approaching the plaintiffs' TPM with a key created by the plaintiffs themselves, and the courts stated that these are not situations that the DMCA was intended to address.[68] These decisions leave two possible ways to avoid liability under section 1201(a): either (1) a person's activities do not constitute circumvention under the statute (as in *I.M.S.*); or (2) a person's activities may fit the definition of the first part of circumvention (descrambling, decoding, avoiding, bypassing, etc.), but because they are authorized to do so, it is not circumvention.

Courts' analyses of the application of copyright-holder-generated passwords and keys begin to falter in cases where the use of a password comes in the more technically sophisticated guise of a software "handshake" that differs from the aftermarket-part context. An example is *Davidson & Associates v. Internet Gateway*, which involved defendants' creation of a server that allowed the playing of a videogame in an alternative "multiplayer" format online with other players but without certain features inherent in the original, and in which some of the players were not "authorized."[69] Though the facts are complicated, the three relevant pieces of software seem to be (1) the videogame itself, purchased by and maintained by the user, (2) the Battle.net server which was run and maintained by plaintiff Blizzard Games, and (3) the bnetd.org server which was run and maintained by defendants,

63. 401 F. Supp. 2d 105, 108 (D.D.C. 2005).

64. The plaintiff was a professor at Brown University, and the username and password for the website were "brown" and "student," respectively. *See id.* at 108 n.4.

65. *Id.* at 113.

66. *Id.*

67. 497 F. Supp. 2d 627, 646 (E.D. Pa. 2007).

68. *See id.* at 644–45 (citing I.M.S. Inquiry Mgmt. Sys. v. Berkshire Info. Sys., 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004)); *Egilman*, 401 F. Supp. 2d at 113–14 (same).

69. 334 F. Supp. 2d 1164, 1168–74 (E.D. Mo. 2004), *aff'd sub nom*, Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005).

independently from plaintiff Blizzard.[70] Because the Battle.net server and the bnetd.org server ran completely independently of each other and did not interact, the concern arose over the authorized use of the Battle.net multiplayer *mode* within the user's copy of the videogame itself.[71]

Defendants claimed they had rightfully purchased a copy of the game, and therefore had the right to use it as they wished.[72] Plaintiff argued that though defendants were authorized to play the game, they did not have the authority to access the game's Battle.net mode via their "fake" bnetd.org server.[73] Essentially, the plaintiff asserted that it was false to assume that "permission to access Battle.net mode via a Battle.net server create[d] implied authority to access Battle.net mode via a fake Battle.net server," here, bnetd.org.[74] The court sided with the plaintiff and found circumvention under the DMCA:

> It is true the defendants lawfully obtained the right to use a copy of the computer programs when they agreed to the EULAs [End User License Agreements] and TOU [Terms of Use]. The statute, however, only exempts those who obtained permission to circumvent the technological measure, not everyone who obtained permission to use the games and Battle.net. The defendants did not have the right to access Battle.net mode using the bnetd[.org] emulator. Therefore, defendants' access was without the authority of the copyright owner.[75]

This decision is counter-intuitive and quite possibly incorrect.[76]

To explain why, we must return to the concept of authorization, asking whether the authorization comes from the purchase of the game or from the EULA. The purchaser of a Blizzard game might like to access all of the features of a game, and might believe he has the ability to do so as he wishes. Under a doctrine of first sale–type analysis, the purchaser would be entitled to do whatever he wanted with his copy of the game.[77] But the doctrine only applies if the purchaser actually gains title to his copy of the game, rather than a license.[78] Moreover, the TOU for Battle.net prohibits reverse engineering and the creation of other emulators.[79] But there is nothing in the EULA that prohibits the *use* of other emulators like bnetd.org.[80]

---

70. *See id.* at 1168–69, 1171–73.

71. *Id.* at 1171–73.

72. *Id.* at 1184.

73. *Id.*

74. *Id.*

75. *Id.* at 1185 (citation omitted).

76. "Given that the opinion as a whole construes breach of contract and anti-circumvention under Section 1201, not copyright infringement under Section 501, it is difficult to resist the notion that a breakdown of categories afflicts this opinion." NIMMER & NIMMER, *supra* note 5, § 12A.04(B)(1) n.44.2.

77. *See* 17 U.S.C. § 109 (2006) (codifying the doctrine of first sale).

78. *Id.*

79. *Davidson & Assocs.*, 334 F. Supp. 2d at 1171.

80. Unless it can be construed from the text "you may not, in whole or in part, copy, photocopy,

However, the district court sided with the plaintiff who claimed "defendants did not have authority to access Battle.net mode via a fake Battle.net server."[81] Thus, the contention is not that Battle.net was being circumvented, but that the videogame's grant of access to the *mode* within the game was circumvented. However, if the purchase of the videogame constituted authorization to play it in whatever mode the purchaser wanted, and the purchaser visited bnetd.org before agreeing to the limiting TOU on the Battle.net site, then presumably the purchaser is authorized to play the videogame in whatever mode he wants. Nimmer notes that once individuals purchased lawful copies of the Blizzard software they could use bnetd.org, but this "was galling to Blizzard, which wanted them to log on solely through the instrumentality of its own proprietary Battle.net."[82] In that sense, this case is another example of a plaintiff trying to control the downstream use of his product, similar to the aftermarket-parts cases.

Furthermore, it seems that the district court and the Eighth Circuit got the CD Key "handshake" protocol confused. The CD Key is contained in the videogame, used by the Battle.net server to verify that it is a legitimately purchased copy, and then allows the videogame to access the multiplayer features of Battle.net.[83] It is, to compare with *I.M.S.*, the password that allows the individual user's copy of the videogame access to the Battle.net server. It is backwards to say that a CD Key that comes with every copy of the videogame software is also used to grant access to a feature within that software itself. But even with that reasoning, the purchaser has a legitimate CD Key, and therefore has the authority vested in the CD Key to access the features of the software. Though defendants may not have been authorized to *reach out to other* Blizzard game owners and access their Battle.net modes, it is hard to see why those same users, initiating contact with the bnetd.org server, could not grant the bnetd.org server authorization to access their copy of the videogame. Enforcement of any other agreements imposed as a result of using the Battle.net service is purely contractual in nature, and should not implicate the DMCA.[84]

---

reproduce, translate, reverse engineer, derive source code, modify, disassemble, decompile, create derivative works based on the Program, or remove any proprietary notices or labels on the program without the prior consent, in writing, of Blizzard." *Id.* at 1170–71 (footnotes omitted) (citation omitted).

81. *Id.* at 1184.

82. NIMMER & NIMMER, *supra* note 5, § 12A.06(C)(2)(c).

83. *Davidson & Assocs.*, 334 F. Supp. 2d at 1169.

84. The court also seems to make an erroneous statement: "It is undisputed that defendants circumvented Blizzard's technological measure, the 'secret handshake' between Blizzard games and Battle.net, that effectively controlled access to Battle.net mode." *Id.* at 1184–85. That is not clear at all, since defendants denied circumvention and only pled for section 1201(f) relief in the alternative. *Id.* Furthermore, because bnetd.org did not communicate with Battle.net in the course of the

Similarly, in the recent case of *Ticketmaster L.L.C. v. RMG Technologies, Inc.*, plaintiff website operator and copyright owner maintained a website with internal pages protected by a lock-out screen, provided the authorized password to access these pages on the lock-out screen itself, freely permitted the use of those internal pages by individuals who accepted the Terms of Service agreement (TOS), and only forbade its use by automated "robots" through that TOS.[85] Defendant created and sold a device that allowed customers to navigate the pages automatically, facilitating faster ticket purchases than ordinarily possible with a single person encountering the "CAPTCHA" system.[86] The court took a creative route to imputing both section 1201(a) and (b) liability to RMG, finding that because users of the device violated the TOS, when the users of RMG's program subsequently navigated the webpages (necessarily copying them to RAM), they then committed copyright infringement.[87] The court further found that the CAPTCHA device protected this right of reproduction, which defendant primarily intended his device to circumvent.[88] Though defendant asserted that "CAPTCHA is designed to regulate ticket sales, not to regulate access to a copyrighted work" (or the right of reproduction), the court rejected this argument without explanation.[89] Arguably, the purpose of Ticketmaster's site is indeed to sell tickets, not to provide exclusive access to its copyrightable descriptions of upcoming performances.[90]

The court here does not adequately analyze the circumvention device at issue or explain how Ticketmaster's "CAPTCHA" system

---

"handshake," it is difficult to see how this might constitute circumvention in the traditional sense. Rather, the game itself is sought permission to play on the bnetd.org server, and the server complied.

85. 507 F. Supp. 2d 1096, 1102 (C.D. Cal. 2007).

86. *Id.* at 1102–03. CAPTCHA is an application that

> presents "a box with stylized random characters partially obscured behind hash marks." The user is required to type the characters into an entry on the screen in order to proceed with the request. Most automated devices cannot decipher and type the random characters and thus cannot proceed to the copyrighted ticket purchase pages.

Id. at 1112 (citations omitted).

87. *Id.* at 1105–10; *see also* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993).

88. *Ticketmaster L.L.C.*, 507 F. Supp. 2d at 1111–12. The court's interpretation of Ticketmaster's copyright infringement claim has staggering implications. The court held that viewing plaintiff's webpages in a browser (and thus storing a copy in RAM), consisted of making copies of those webpages within the copyright right of reproduction. *Id.* Next, Ticketmaster's TOS grants a license to users who want to view (and thus, according to the court, copy) its copyrighted pages. *Id.* Finally, the court held that when users violated the terms of service and continued to navigate the webpages, it committed copyright infringement. *Id.* This implies that anyone who violates a similar TOS and continues to browse is liable for copyright infringement; a shocking proposition in the Internet age.

89. *See id.* at 1112.

90. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 549 (6th Cir. 2004) ("Nowhere in its deliberations over the DMCA did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumer goods while leaving the copyrightable content of a work unprotected.").

effectively protects access to the work. First, it is not clear from the facts whether defendant's device identifies the password in the CAPTCHA and applies it as any ordinary user would, or whether it employs some more nefarious "hacking" tool to decrypt the correct answer. If defendant's device simply identifies the password in the CAPTCHA and applies it, the device's actions do not fit the definition of circumvention under either subsection of section 1201.[91] Second, and perhaps more importantly, the court ignores the Sixth Circuit *Lexmark* decision which held that a device that did not actually protect or prevent anyone from reading the copyrighted material did not effectively control access.[92] Here, the password was displayed on the lockout screen, clearly visible to any user, and the content of the copyrighted pages behind the lockout screen were made freely available.[93] It is therefore questionable whether the CAPTCHA device effectively protected a work under section 1201.

Another flaw in the decision, as many others before it, is that the court did not adequately examine the issue of authorization in its section 1201(a) analysis. For the purposes of the DMCA, where should the court have looked for "authority"? The TOS explicitly said that automated devices were prohibited, but that is a tenet of contract law, the violation of which should not necessarily trigger revocation of authorization or DMCA liability.[94] Moreover, the TOS applied only after the lockout screen was passed and Ticketmaster made the password publicly available,[95] which essentially authorized anyone who could read it. While click-wrap agreements like the TOS here are valid contracts in theory, any user would glean an implicit authorization to use the website from the free availability of the password.[96] Lastly, the court did not specifically address whether a technological measure can block automated access but not manual access and yet still be an "effective" measure under the DMCA. Because the DMCA does not distinguish between manual users and automated users, and because the

91. Of course, if defendant's device does the latter, the court's DMCA analysis is largely correct.

92. *See* discussion *supra* Part III.

93. *Ticketmaster L.L.C.*, 507 F. Supp. 2d at 1105, 1112.

94. *See* Lipton, *supra* note 44, at 490 ("Congress did not intend to impact significantly the usual rules and policies relating to commercial competition in tangible goods. These rules and policies generally are provided by contract, supplemented by legislation and case law dealing with commercial transactions, and also regulated to a significant extent by antitrust laws."). *But see* Orin S. Kerr, *A Lukewarm Defense of the Digital Millennium Copyright Act*, *in* COPY FIGHTS: THE FUTURE OF INTELLECTUAL PROPERTY IN THE INFORMATION AGE 163, 167 (Adam Thierer & Wayne Crews eds., 2002) (stating that the goal of the DMCA is "to stop people from breaching their contracts by interfering with the market for contract-breaching tools. . . . The idea is . . . you can help make contracts enforceable by deterring people from making and distributing contract-breaching devices.").

95. *See Ticketmaster L.L.C.*, 507 F. Supp. 2d at 1102, 1107, 1112.

96. *See, e.g.*, Sprecht v. Netscape Commc'ns Corp., 306 F.3d 17, 21–25 (2d Cir. 2002); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449–50 (7th Cir. 1996); Ticketmaster, Corp. v. Tickets.com, Inc., No. CV 99-7654, 2000 WL 525390, at *3 (C.D. Cal. Mar. 27, 2000).

authorization is implicit before the TOS is accepted, and is only revoked by contract violation after, the court's decision is incomplete. These two decisions show why courts' varying definitions of the term "authorization" should be revisited. The next Part will further demonstrate why this is so.

IV. THE EFFECTS OF IMPRECISELY DEFINING "AUTHORIZATION" IN THE DMCA

"The notion of authorization is central to understanding section 1201(a)."[97] As the preceding cases demonstrate however, courts have not sufficiently or consistently addressed the definition of "authorization" in their analysis of alleged DMCA violations. Similarly, because courts have failed to consistently define it within the Computer Fraud and Abuse Act of 1986 ("CFAA") and other state computer fraud statutes,[98] it is instructive to examine proposed treatment of the term there.[99]

A. THE DEFINITION OF "AUTHORIZATION" IN THE CFAA CONTEXT

The CFAA addresses computer fraud, providing civil and criminal penalties to those who, among other things, access a computer "without authorization" or who "exceed[] authorized access" to a computer.[100] Common violations include "computer hacking, distribution of computer worms and viruses, and denial-of-service attacks."[101] More so than the DMCA, the CFAA imputes liability for the acts of trespass and fraud that evoke a "lock and key" analogy because the crimes typically involve a person breaking into a computer that is owned by someone else, thereby invading his or her "property."[102]

In his discussion of authorization, Professor Kerr points out that computer crimes statutes generally do not define the phrase "without authorization,"[103] and that the cases interpreting them have given varied definitions.[104] The first of these definitions is the "intended function" test for authorization, which states "[w]hen a user exploits weaknesses in a program and uses a function in an unintended way to access a computer . . . that access is without authorization."[105] The second set of cases Kerr describes adopted an agency definition of authorization derived from the *Restatement (Second) of Agency*, whereby employees

97. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1202 (Fed. Cir. 2004).

98. Orin S. Kerr, *Cybercrimes' Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1598 n.11 (2003).

99. *Id.* at 1599.

100. 18 U.S.C. § 1030 (2006).

101. Kerr, *supra* note 98, at 1603–04.

102. *See id.* at 1609–11.

103. *Id.* at 1623–24.

104. *Id.* at 1628.

105. *Id.* at 1632.

are authorized until they begin acting as agents for someone other than their employer.[106] Kerr notes that some of these cases embody a "strikingly broad" theory of agency, whereas other cases that also take into account the intent of the employee to exceed access are "slightly narrower."[107] The third category of authorization, according to Kerr, involves contractual provisions.[108] Surprisingly, at least in civil cases, authorization is exceeded when a contract explicitly defining authorization is breached.[109] This last interpretation, as will be discussed below, appears in the DMCA context as well, and there, as here, allows for the possibility that "[n]early any use of a computer that is against the interests of its owner is an 'access' . . . triggering severe criminal penalties."[110]

Kerr outlines two possible approaches to computer fraud and misuse cases: define unauthorized access based either on contract or on restrictions by code.[111] He then proposes a single interpretation of both "authorization" and "access" based on the latter approach.[112] Essentially, Kerr suggests a broad interpretation of the word "access," to include any "successful interaction" within the statute,[113] and a limited definition of the phrase "without authorization" that would include only circumvention of restrictions by code.[114] Kerr argues that "[b]y granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner."[115] In reining in this excessive power, he attempts to "mediate the line between openness on the one hand, and privacy and security on the other."[116]

---

106. *Id.* at 1632–33 (discussing Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000)).

107. *Id.* at 1633–34.

108. *Id.* at 1637.

109. *Id.*

110. *Id.* at 1640. Kerr further notes that "[c]ourts previously used harm as a proxy for theft; now they appear to use harm as a proxy for lack of authorization." *Id.* at 1642.

111. *See id.* at 1599–1600.

112. *Id.* at 1642.

113. *Id.* at 1646–47.

114. *Id.* at 1648–49 ("When a user circumvents regulation by code, she tricks the computer into giving her greater privileges . . . . This normally can occur in two ways. First, a user can enter the username and password of another user with greater privileges . . . . Second, a user can exploit a design flaw in software that leads the software to grant the user greater privileges . . . . In contrast, when a user breaches a regulation by contract, the user need not trick the computer: The user need only take steps that breach a condition of the use imposed by the computer owner." (footnotes omitted)).

115. *Id.* at 1651. As the next section discusses, courts have similarly delegated this rulemaking authority to copyright owners under the DMCA.

116. *Id.* at 1650. Similarly under the DMCA, the balance should be between protecting the rights of the copyright owner and protecting the interests of the consumer of the copyrighted work. For in the case of many a copyrighted work, under the DMCA the copyright owner is simultaneously selling access and taking it away with code-based restrictions. Susan Brenner has also expressed concern

Though Kerr contends that his advocacy of liability based on the circumvention of a code-based restriction in the CFAA context does not carry over into the DMCA,[117] it is instructive to consider how different definitions of authorization might affect DMCA cases. Courts at the very least should acknowledge the possible distinctions. While courts have generally made the right determinations in the clearer cases, the exceptions demonstrate that rather than explain why they have chosen to impute a particular level of authorization, courts have often looked to the preferences of the copyright owner to determine whether there was authorization.[118] This lack of detailed analysis of the authorization requirement can pose a risk to acceptable uses of devices ostensibly allowed under the DMCA.[119] Because of the current inconsistency in defining "authorization" under the DMCA, settling on either a broad or narrow definition of authorization in assessing alleged circumvention under section 1201(a) would lead to different rulings than courts have made in many cases so far. The next two subsections illustrate this inconsistency.

B. The Effect of Using a Permissive Definition of Authorization

Giving the most permissive interpretation to the term "authorization" in section 1201(a)(3), subsections (A) and (B), and "circumvention" in section 1201, subsections (a) and (b), would require the reversal of many DMCA cases. On this definition, as in the aftermarket-parts and password cases, the existence of a password or key issued by the copyright holder would constitute authorization to access the work behind the TPM through use of that password or key, and would thus not constitute circumvention.

---

about the "criminalization" of the dissemination of information. She explains:

> Posting code is a much more ambiguous act than selling the combination to a bank safe.
>
> . . . .
>
> The DMCA criminalizes the dissemination of technical/scientific information that can be used to compromise technology that protects copyrighted material. It criminalizes the distribution of this information even though (a) it does not "belong" to the parties who own the copyrights and (b) it can have expressive content, the distribution of which may facilitate technical and scientific inquiry. The DMCA criminalizes the dissemination of the information it encompasses on the premise that it can be used to facilitate copyright infringement. It is a pure "burglar's tools" statute.

Susan W. Brenner, *Complicit Publication: When Should the Dissemination of Ideas and Data Be Criminalized?*, 13 ALB. L.J. SCI. & TECH. 273, 347, 403 (2003) (footnotes omitted).

117. Kerr, *supra* note 98, at 1651 n.239.

118. *See supra* Parts I, III.

119. Professor Denicola notes that "superficial judicial analysis of the distinction has occurred mostly in trafficking cases, where the difference between access and rights controls is essentially irrelevant. The risk, of course, is that this nonchalance will spill over into circumvention cases, where the distinction is crucial to the balance envisioned by Congress." Robert C. Denicola, *Access Controls, Rights Protection, and Circumvention: Interpreting the Digital Millennium Copyright Act to Preserve Noninfringing Use*, 31 COLUM. J.L. & ARTS 209, 220–21 (2008).

For example, for purposes of DMCA liability only (not contractual liability), if the authorization for accessing the inner pages of Ticketmaster's website came from the public display of the CATPCHA password on the screen, then defendant's device in *Ticketmaster* would not have circumvented the TPM. This is because the application of information would properly encounter the TPM, not "descramble, decrypt," etc.,[120] within the first criterion of section 1201(a). Even if it did, any decryption would have been achieved with the "authority of the copyright owner."[121] Similarly, in *Davidson*, if the authorization to play the videogame comes from the sale of the single-player game to consumers, then it is improper for Blizzard to use the DMCA to prevent the use of a portion of its game in a way Blizzard would prefer it not to be used. This case seems similar to the aftermarket-parts cases, for recall in *Storage Technology*, "courts generally have found a violation of the DMCA only when the alleged access was intertwined with a right protected by the Copyright Act."[122] Thus, even if the use of defendant's bnet.org server to access the videogame's Battle.net multiplayer mode was unauthorized, *Davidson* would be incorrect because there is no evidence that the copyrighted material in the videogame was subject to copying or violation of any other rights of copyright.

At the most extreme reevaluation, the DeCSS cases would require further consideration as well. For example, according to descriptions of DeCSS's creation, an initial key was left unencrypted.[123] The copyright holder had legitimately issued this key.[124] The creators of DeCSS obtained this unencrypted key and were able to guess the others, as the password was likely guessed in *Egilman*.[125] Though the creators in essence "stole" the key, this is no different from the actions of the defendants in *I.M.S.* who escaped DMCA liability.[126] If instead, one of the DVD player manufacturers had given the creators of DeCSS the key, it is possible that whatever implicit authorization was possessed by the

120. 17 U.S.C. § 1201(a) (2006).

121. *Id.* § 1201(a)(3).

122. 421 F.3d 1307, 1318 (Fed. Cir. 2005).

123. Patrizio, *supra* note 24 ("To descramble the video and audio, a 5-byte (40-bit) key is needed. Every player—including consoles from Sony, Toshiba, and other consumer electronics vendors, as well as software vendors for PCs like WinDVD and ATI DVD—has its own unique unlock key.... All licensees of DVD technology have to encrypt their decryption key so no one can reverse-engineer the playback software and extract the key. Well, one licensee didn't encrypt their key. The developers of DeCSS, a Norwegian group called MoRE (Masters of Reverse Engineering) got a key by reverse-engineering the XingDVD player, from Xing Technologies, a subsidiary of RealNetworks.").

124. *Id.*

125. *Id.*; *see also* discussion of *Egilman*, *supra* Part III.

126. *See* 307 F. Supp. 2d 521, 533 (S.D.N.Y. 2004) ("Plaintiff authorized someone else to use the DVD player, and defendant borrowed it without plaintiff's permission. Whatever the impropriety of defendant's conduct, the DMCA and the anti-circumvention provision at issue do not target this sort of activity.").

DVD manufacturer was passed on to the DeCSS makers. Then the only thing that might arguably stand in the way is the licensing agreement between the DVD player manufacturer and the copyright holder. However, the *Chamberlain* court and other commentators have said the DMCA should not be used to enforce these agreements.[127] Does a copyright holder have to "authorize" every transfer of a validly-issued password or key before its use ceases to be circumvention under the DMCA?

In light of this discussion, it is possible to read *321 Studios* as a password case that was wrongly decided in part. There the court failed to address three issues: (1) whether the use of an authorized "key" can confront a TPM and not circumvent under the DMCA, (2) the definition of "authorized by the copyright holder," and (3) that authorization by the copyright holder does not implicate liability under section 1201(b).

While the specific issue was not raised in *321 Studios*, there are many ways for DVD player manufacturers and other users to have obtained the unencrypted key for CSS and use it in a way that would be consistent with *I.M.S.* The question is, can a more technologically sophisticated key be held to properly confront a measure such that it does not circumvent, like a password can? Both password and keys are used to "unlock" TPMs. They are arguably the same. Unfortunately, neither Congress nor the courts have articulated the crucial distinction between a password (typically typed by a human), and an automated or software-based "handshake" key.

Another argument is that the different decisions reflect how courts look to the attendant conduct to decide whether the use was allowable. For example, in *Egilman*, the plaintiff did not accuse the defendant of depriving him of a sale or of infringing upon his right of distribution. Indeed, plaintiff was not offering the information for sale; it was kept on his own website for academic dissemination and he clearly preferred to keep it secret.[128] Therefore, the conduct was more akin to computer fraud, thereby not implicating the DMCA as heavily as in a case like *Corley*, where it was shown that the makers of DeCSS were encouraging copyright infringement.[129]

The second issue with *321 Studios* surrounds the meaning of "authorized by the copyright holder." The DMCA does not define "authorization," and the court in *321 Studios* does not address it. Plaintiffs essentially claimed defendants did not have "authority" because they did not license the player key through the proper

127. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1202 (Fed. Cir. 2004) ("What the law authorizes, Chamberlain cannot revoke."); Reichman et al., *supra* note 4, at 1028.

128. Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105, 108 (D.D.C. 2005).

129. 273 F.3d 429, 439 (2d Cir. 2001).

channels.[130] Giving effect to the *321 Studios* construction of section 1201 would imply, in a way not contemplated by Congress, that the owner of a DVD needs authorization to use the DVD, because use requires decryption. For example, imagine that a DVD manufacturer not in a license agreement with the copyright holder obtains a valid key from another manufacturer and uses it in its player.[131] It would be nonsensical to hold the owner of a legitimately purchased DVD liable for circumventing section 1201(a) because he or she used the player, simply because the player did not have a contract with the copyright holder. As commentators have noted, there are considerable antitrust concerns implicated when copyright owners are able to dictate all of the downstream uses of their works, as well as the media upon which it is stored.[132]

The third and final problem with the *321 Studios* decision is the reference to authorization in the court's assessment of section 1201(b) liability. Under section 1201(b) of the DMCA, "to 'circumvent protection afforded by a technological measure' means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."[133] The court in *321 Studios* erroneously dismisses, without discussion, the fact that this definition does not state that lack of authorization from the copyright holder will trigger liability. Unlike provisions of section 1201(a) that govern "access," section 1201(b) is intended to address technological protection of the rights afforded by the Copyright Act and only addresses devices made to circumvent them. Thus, circumvention is only committed within the meaning of section 1201(b) by avoiding bypassing, removing, deactivating, or otherwise impairing.[134] Therefore, if the player key is a valid "password" authorized by the copyright holder, according to *I.M.S.* and *Egilman* the application of said key would not constitute circumvention under section 1201(b) because it would properly confront the TPM, not circumvent it.[135]

In contrast, the *321 Studios* court simply stated that, "while 321's software does use the authorized key to access the DVD, it does not have authority to use this key, as licensed DVD players do, and it therefore

130. 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1094–95 (N.D. Cal. 2004).

131. Also assume that the player does not enable copying, so as not to run afoul of the provisions of section 1201(b).

132. Reichman et al., *supra* note 4, at 1028.

133. 17 U.S.C. § 1201(b)(2)(A) (2006).

134. Reichman et al., *supra* note 4, at 1028.

135. *See* Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105, 113 (D.D.C. 2005) ("[U]sing a username/password combination as intended—by entering a valid username and password, albeit without authorization—does not constitute circumvention under the DMCA."); I.M.S. Inquiry Mgmt. Sys. v. Berkshire Info. Sys., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004) (noting that "defendant is not said to have avoided or bypassed the deployed technological measure in the measure's gatekeeping capacity").

avoids and bypasses CSS."[136] With this, the court attempts to separate the authorization of the key from the authorization of the actor. Furthermore, it uses the definition of circumvention from section 1201(a) to impute liability under section 1201(b). While the defendant here might be liable under section 1201(a) if its use of the key was not authorized (leaving aside for a moment what constitutes the authorization of the copyright holder), section 1201(b) is drafted differently. As opposed to section 1201(a), section 1201(b) does not mention authorization at all, so the lack of it alone cannot constitute circumvention under that section.[137] Under section 1201(b), if defendants are using an authorized key in the manner intended, such that their conduct does not constitute "avoiding, bypassing, removing, deactivating, or otherwise impairing," following the *I.M.S.* standard, it should not matter whether or not they were authorized.[138]

C. The Effect of Using a Restrictive Definition of Authorization

While defaulting to a permissive definition of "authorization" may not make sense in all contexts, there are policy and common sense reasons for not applying a restrictive definition, and for not allowing the "avoid, bypass" terminology in section 1201(a) to reach all cases. Scholars have argued that it would be "absurd and disastrous" to construe section 1201(a) as being "concerned only with control over access, and not with rights protected by copyright law," because:

> It would "allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial 'encryption' scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products." This would "allow virtually any company to attempt to leverage its sales into aftermarket monopolies," even though this would be unlawful under the antitrust laws and the copyright misuse doctrine.[139]

As Professor Kerr asks in the CFAA context, "who and what determines whether access is authorized . . . . Can a computer owner set the scope of authorization by contractual language? Or do these standards derive from the social norms of Internet users?"[140] As the alternative outcomes of the following cases will demonstrate, requiring express authorization

136. 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004).

137. *Compare* 17 U.S.C. § 1201(a)(3)(A) (defining circumvention as certain actions "without the authority the copyright owner"), *with id.* § 1201(b)(2)(A) (defining circumvention without any such authorization element).

138. *Id.* § 1201(b)(2)(A).

139. Reichman et al., *supra* note 4, at 1028 (footnotes omitted) (quoting Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1201 (Fed. Cir. 2004)).

140. Kerr, *supra* note 98, at 1623.

from the copyright holder would not always be feasible, desirable, or possible.

The decisions in *I.M.S.* and *Egilman* might not have come out differently under a narrow, express authorization requirement, because both courts found that the actions of the defendants did not meet the first part of section 1201(a)(3)(A), namely that the application of the passwords did not descramble, decrypt, avoid, bypass, remove, deactivate, or impair the TPM.[141] However, if the courts had determined that the defendants' actions were "deactivations" of the measures, the next question would be whether defendants' use of the valid password was "authorized." If not, the plaintiffs in these cases would probably have succeeded on their DMCA claims.

Consider, also, the aftermarket-parts cases. If the Federal Circuit in *Chamberlain* and *Storage Technology* had held that the plaintiffs had not given authorization to access the copyrighted material in garage door openers and data storage libraries, the kind of monopolies the court suggested might result. This would have further rippling effects as more and more devices are embedded with copyrightable software program, and the fears of widespread use of "trivial encryption schemes" and unintended monopolies described by the scholars quoted above would be realized.

Finally, decisions in cases like *Ticketmaster* and *Davidson* would become more common in areas further and further divorced from the purposes of copyright law or the DMCA. As discussed above, the *Ticketmaster* decision has surprising implications because it allows copyright holders to appear to make their work available while imposing virtually any condition upon that access. This is hardly the benefit to society that the Copyright Act envisions providing. It further makes merely browsing the Internet in certain contexts a violation of copyright law.[142] Companies like the plaintiff in *Davidson* would continue to be able to control the downstream use of software like videogames, even after they obtain the benefit of the sale.

As these cases illustrate, various problems arise if we require express authorization from the copyright holder. First, although the DMCA has existed for over a decade now, consumers are still accustomed to being able to do what they want with items they have rightfully purchased. The First Sale Doctrine is firmly rooted in our collective consciousness, as partially demonstrated by the resistance to digital rights management programs in legally purchased copies of copyrighted works.[143] "As the

141. *See supra* notes 60, 66 and accompanying text.

142. *See generally* Matt Jackson, *Using Technology to Circumvent the Law: The DMCA's Push to Privatize Copyright*, 23 HASTINGS COMM. & ENT. L.J. 607 (2001).

143. For example, this is seen in cases that deal with regional coding on video games and DVDs.

Chamberlain and *Lexmark* cases both demonstrate, consumers and commercial competitors may have very different normative expectations from an original product manufacturer about what conduct is appropriate with respect to the product in an after-market context."[144] Moreover, Professor Lipton notes the "increasing judicial concerns about protecting the reasonable expectations of the average consumer .... Surely consumers must have an implicit right to buy a product that will enable them to utilize their garage door openers."[145] While this argument is only made explicit in the aftermarket-parts context, it seems correct that the "reasonable expectations of the average consumer" should be respected in other contexts too. To use the DMCA to forbid people to share what they have legally purchased with their family or friends is an affront to this principle.

It is also important to recall the Federal Circuit's holding in *Storage Technology*, which reiterated that because the DMCA is intended to help protect rights of copyright, and not of contract, the DMCA should not be used to enforce contractual restrictions.[146] Furthermore in *Chamberlain*, the court noted the need to avoid a construction of the DMCA that would "allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work."[147] Otherwise, copyright holders can enforce their will, through increasingly complicated licenses and technological measures, and have it supported by the DMCA. This is precisely what will occur, however, if the authorization prong is interpreted in this narrow fashion.

See Denicola, *supra* note 119, at 224–25 ("A district court issued a preliminary injunction against the sale of a device that circumvented similar regional coding used by Sony on its PlayStation video games, holding that regional coding was an access control. This too seems wrong.... [O]wners of regionally-coded games have authorized access to the entire copyrighted expression contained in their copy. Unlike CSS, regional coding ... does nothing to inhibit the copying of games or DVDs. Copyright owners might argue that the coding assists in protecting their exclusive right 'to distribute copies or phonorecords of the copyrighted work to the public.' However, only a 'technological measure that effectively protects a right of a copyright owner under this title' is entitled to protection under § 1201(b). The 'first sale' doctrine in § 109 of the Copyright Act grants the owner of a lawfully made copy of a copyrighted work the right to sell or otherwise dispose of possession of that copy. Thus, the Copyright Act does not give the movie studios the right to control the subsequent redistribution of lawfully made DVDs, and hence a technological attempt to safeguard that interest does protect a right of the copyright owner under Title 17. Neither the anti-circumvention nor the anti-trafficking rules would then be applicable to regional coding." (footnotes omitted)).

144. Lipton, *supra* note 44, at 514.

145. *Id.*

146. *See* 421 F.3d 1307, 1319 (Fed. Cir. 2005) ("The activation of the maintenance code may violate [Storage Technology's] contractual rights vis-à-vis its customers, but those rights are not the rights protected by copyright law. There is simply not a sufficient nexus between the rights protected by copyright law and the circumvention of the GetKey system.").

147. 381 F.3d 1178, 1202 (Fed. Cir. 2004).

Another problem with enforcing an express authorization requirement and broad definition of circumvention is that "today . . . everything is protected by copyright and it is almost impossible to figure out whom to ask for permission."[148] Thus, it is impossible to know whom to ask for authorization to share one's password, DVD player key, etc., or to circumvent a rights control device for a fair use purpose. Additionally, even if one knew where to seek authorization, there is no guarantee copyright holders will grant it. This is especially true in cases where they perceive a risk to their own interests, even if copyright law would condone the desired use or access in the absence of the DMCA.[149] For example, "[b]y using TPMs, copyright owners arguably gain the power to opt out of those parts of the copyright system they dislike. They can not only design TPMs to circumvent public interest uses, but can claim shelter behind section 1201 for doing so."[150] Furthermore, "there is as yet no incentive for copyright owners or TPM vendors to fine-tune TPMs to enable non-infringing uses."[151] The *Chamberlain*, *Storage Technology*, and *Lexmark* cases demonstrate attempts to corner markets that Congress did not intend to protect. Additionally, Professor Reese has noted the increasing popularity of TPMs that "merge" access and rights controls, giving copyright owners the extra protection of the authorization component of section 1201(a), even in a rights control situation.[152] The danger here is that "copyright owners can use these technological measures not only to prevent infringement, but also to avoid the limitations that copyright law places on their monopoly privilege."[153] Therefore, in the absence of a clear enough definition of authorization in these gray area cases, it behooves courts to apply the DMCA circumvention terms carefully rather than go beyond the intent of Congress to the detriment of consumers and fair use.

An additional risk of restrictively interpreting the term "authorization" is that it will stifle the newsgathering process or restrict access to material that a user is actually entitled to see. This risk has already manifested itself at least one instance. In 2002, reporter Declan

148. Jessica Litman, *Sharing and Stealing*, 27 HASTINGS COMM. & ENT. L.J. 1, 22 (2004).

149. *See* NIMMER & NIMMER, *supra* note 5, § 12A.06(C)(2)(c); *see also* Burk, *supra* note 1, at 1106.

150. Reichman et al., *supra* note 4, at 1023.

151. *Id.*

152. *See* Reese, *supra* note 4, at 621 ("Copyright owners may instead be able to employ technological protection systems that incorporate both an access control and a rights control. So far, courts have treated such 'merged' control measures as entitled to the legal protections of *both* access- and rights-control measures, even when the system was essentially directed only at preventing copying and distribution, rather than at controlling access. . . . The deployment of merged control measures thus poses a threat to the congressional scheme for balancing protections for copyright owners against the public's interest in noninfringing use.").

153. Jackson, *supra* note 142, at 615.

McCullagh obtained the username and password to a government website that purported to contain information about airport security procedures and the relationship between federal and local police.[154] Because the information claimed to be "restricted to airport management and local law enforcement," McCullagh feared prosecution from using the legitimate password given to him by someone else.[155]

Fortunately, the cases that address the application of manual passwords, *I.M.S.* and *Egilman*, have shown that McCullagh's actions would not likely be considered circumvention. But cases like *Davidson* imply they might, if the original recipient has agreed to some contractual restriction against sharing. There is a danger if the commentators who disagree with the *I.M.S.* line of cases have their way. Letting courts use DMCA liability to enforce contractual provisions, rather than enforcing the provisions themselves, enables copyright owners to extract greater civil penalties, and in some instances impose criminal liability, where contract law would not otherwise provide such a remedy.[156] "[T]he DMCA's operation should be restricted to disputes that are really about digital copyright piracy."[157]

V. PROPOSED REMEDY

What all of the cases above illustrate is that a failure to clearly define authorization has resulted in confusion and inconsistency. Restrictive interpretation of the circumvention provision, especially the term "authorization," leads to illogical case law and possibly unfair outcomes. Thus Congress or the courts should better define what constitutes "authorization" under sections 1201(a)(3)(A) and 1201(a)(3)(B) of the DMCA, and clarify how this differs from the definition of circumvention under section 1201(b), in order to more clearly demarcate what conduct is permitted and what is forbidden.[158] Otherwise, as the aftermarket-parts cases demonstrate, plaintiffs may claim lack of authorization when someone does something with their work that they simply dislike.[159] Or,

154. Declan McCullagh, *Perspective: Will This Land Me in Jail?*, CNET NEWS, Dec. 23, 2002, http://www.news.com/2010-1028-978636.html.

155. *Id.*

156. *Cf.* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1201 (Fed. Cir. 2004) ("Under Chamberlain's proposed construction . . . disabling a burglar alarm to gain 'access' to a home containing copyrighted books, music, art, and periodicals would violate the DMCA; anyone who did so would unquestionably have 'circumvented a technological measure that effectively controls access to a work protected under [the Copyright Act].' The appropriate deterrents to this type of behavior lie in tort law and criminal law, *not* in copyright law.").

157. Lipton, *supra* note 44, at 515.

158. *See* 17 U.S.C. § 1201(a)(3)(A)–(B), (b) (2006).

159. As Professor Ginsburg notes, copyright holders have already made a bad name for themselves, and are as equally guilty of hyperbole as the "information wants to be free" set through gambits such as the "over-depiction of 'piracy' as the unauthorized copying by end-users," which "not only distorts but trivializes the term." Jane C. Ginsburg, *How Copyright Got a Bad Name for Itself*, 26

conversely, courts like the one in *321 Studios* may continue to conflate the issue of authorization with circumvention and possible interference with the rights of the copyright holder, granting more protection to the traditional rights of copyright than Congress intended.[160]

There are many ways to reword the statute to make it easier to apply, while hewing to the original purpose of the DMCA. For example, Professor Samuelson has advocated adding the phrase "or other legitimate purposes" to the anti-circumvention provisions in section 1201(a)(3)(A) to add "flexibility, adaptability, and fairness to the law."[161] This would have the added benefit of more closely mimicking the flexibility of the exceptions of the Copyright Act, because, as she notes, there are in fact legitimate reasons for bypassing access controls.[162] Alternatively, *Nimmer on Copyright* advocates replacing "without the authority of the copyright holder" in section 1201(a)(3)(A) with "unless the person who engages in that conduct has been authorized by the copyright owner to descramble, decrypt, or otherwise to avoid, bypass, remove, deactivate, or impair the technological measure on that work."[163] Because of the ambiguity in the current wording, this change would "follow the chief legislative goal underlying this amendment: augmenting the rights of copyright owners without contributing to a pay-per-use world."[164]

It is easy to argue that stealing or using stolen passwords might be a violation of the statute, but the few cases that have addressed it hold otherwise.[165] A more complicated question arises when passwords are borrowed or shared.[166] If I share my password with someone, is that a violation of the DMCA?[167] Should it be? What if I forget my password?

COLUM. J.L. & ARTS 61, 63 (2002).

160. *See* discussion of *321 Studios*'s analysis of § 1201(b), *supra* Part IV.

161. Pamela Samuelson, *Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 546 (1999).

162. *Id.*

163. NIMMER & NIMMER, *supra* note 5, § 12A.06(D)(2). Nimmer notes that this is one of two alternative interpretations of "without the authorization of the copyright owner" in § 1201(a)(3)(A). The other, "in any manner other than one that the copyright owner has authorized that person to undertake" is much more restrictive and would capture a person "whenever he acts in a manner of which the copyright owner has not approved in advance." *Id.*

164. *Id.*

165. This kind of action is probably more appropriately pursued under a fraud regime such as the CFAA. *See* 18 U.S.C. § 1030 (2006).

166. Litman, *supra* note 148, at 5 (discussing in the Internet context that "[s]omeone knows what I want to know. Someone has the information I want. If I can find her, I can learn it from her. She will share it with me."); *see also id.* at 8 ("[P]eople like to look things up, and they want to share.").

167. Though *I.M.S.* concluded the answer is no, Professor Ginsburg disagrees: "Entry of the password 'deactivates' the measure that restricts access; if the password is employed by an unauthorized user, then the deactivation will not have occurred with the copyright owner's authority." Ginsburg, *supra* note 3, at 27–28 (citations omitted); *see also* Ginsburg, *supra* note 19, at 140 (arguing that a stricter definition probably applies: "in theory, . . . I cannot communicate my password to a

One group of scholars has suggested that "courts could decide that persistent access controls, such as CSS, are not the kinds of 'access controls' that section 1201(a) actually regulates," because CSS is primarily a copy control device that is governed by section 1201(b).[168] This would open up considerably more room for fair use circumventions.[169] "[Courts] could also find in section 1201(c)(1) a statutory basis for excusing fair use circumventions."[170] Perhaps password sharing should be a fair use exception to section1201(a)(1).

Another possibility is to incorporate some of the language of authorization from section 117 of the Copyright Act, which states that "it is not an infringement for the owner or lessee of a machine to make or authorize the making of a copy of a computer program" in certain circumstances having to do with maintenance or repair, and under certain conditions, such as requiring the copy to be destroyed when the work is completed.[171] Similarly, if a consumer has legitimately purchased the rights to use a copyright work, there should be some circumstances where that person can share any necessary password or key with others in a way that "authorizes" the recipient of the password to use it without any DMCA circumvention liability. Professor Reese gives a plausible example:

> What of a device that allows a person to take a DVD "tethered" to her home DVD player and play it on a different DVD player in a friend's home? Arguably, that device has the use of circumventing a technological measure that interferes with lawful activity—privately performing a copyrighted motion picture—rather than (or in addition to) circumventing a technological measure that protects a right of the copyright owner.[172]

Even DMCA supporters acknowledge that "fairness may depend on the nature of the access control: what is the copyright owner seeking to prohibit? In theory, access controls are designed to protect a business model based on price discrimination according to intensity of use."[173] Thus, at the very least in the case of an unlimited-use purchase, circumvention should be permissible.

Perhaps the best solution, then, is for all courts to adopt the reasoning of the Federal Circuit in demanding a "nexus" between the DMCA and actual copyright infringement, because it gives a "framework

---

friend or family member to play the game on my computer, since the password protects access to the work, and my disclosure of the password is an act that circumvents a protective measure that had limited access to me").

168. Reichman et al., *supra* note 4, at 1008.

169. *Id.*

170. *Id.* at 1009.

171. 17 U.S.C. § 117(c) (2006).

172. Reese, *supra* note 4, at 630.

173. Ginsburg, *supra* note 1, at 130.

for interpreting section 1201 that enables courts to develop a balanced approach to interpretation of the DMCA's anti-circumvention rules insofar as copyright owners try to use them to block fair and other non-infringing uses of technically protected copyrighted works."[174] A more nuanced rule would answer the concerns of commentators who contend that an access right is necessary to promote the availability of copyrighted works in digital form. This rule would state that the DMCA is only inapplicable in cases where "circumvention of an access control measure neither substitutes for purchase of the protected work nor creates risk of copyright infringement."[175] Thus, circumvention to avoid paying for access to the copyrighted work would still be forbidden, but gaining repeat access to a work once legitimately purchased, perhaps to experience it on a variety of platforms (and possibly including a "fair use" of sharing one's password) would be permitted.[176]

A final, helpful clarification would be for Congress to clarify the distinction between human and computer actors, if they intended one to exist. Courts like the one in *I.M.S.* have held that the entry of a password manually by a human generally does not circumvent, though commentators have disagreed.[177] Conversely, the *Ticketmaster* court held that the plaintiff website could discriminate between human and computer actors, imputing DMCA liability to one but not the other.[178] But the DMCA does not state whether humans and software code or computers created by humans should be treated differently or similarly. If Ticketmaster is allowed to forbid computers from using its site but not people, or if a software "key" is different from a manually applied "password," Congress should explain the distinctions.

CONCLUSION

"As intellectual property is implicated increasingly in relevant disputes, particularly in the context of detailed intellectual property licenses purporting to impose restrictions on licensees, it becomes

174. Reichman et al., *supra* note 4, at 1032. The aftermarkets parts cases are the one area where courts have engaged in sufficient discussion of authorization. For example, the *Chamberlain* court stated that:

> The plain language of the statute . . . requires a plaintiff alleging circumvention (or trafficking) to prove that the defendant's access was unauthorized—a significant burden where, as here, the copyright laws authorize consumers to use the copy of Chamberlain's software embedded in the GDOs that they purchased. The premise . . . is that the copyright laws authorize members of the public to access a work, but not to copy it. . . . [P]laintiffs must prove unauthorized access.

381 F.3d 1178, 1193 (Fed. Cir. 2004).

175. Denicola, *supra* note 119, at 231.

176. *See, e.g.*, Reese, *supra* note 4, at 660 n.131; Samuelson, *supra* note 4, at 539.

177. *See, e.g.*, Ginsburg, *supra* note 3.

178. *See* 507 F. Supp. 2d 1096, 1102, 1112 (C.D. Cal. 2007).

imperative that we resolve some of these confusions."[179] Granted, so many words are used to describe the definition of "circumvention" in section 1201 because it is a difficult concept to capture, and the ways in which people use technology are constantly evolving. However, Congress should now strive to apply the improved vocabulary that has developed over the past ten years since the original passage of the DMCA to describe what new rights it actually intends copyright owners to have in the digital age. Any new definition should carefully consider the logical consequences of stretching the definition of "authorization" too far in either direction. Without a coherent scheme, it becomes too easy for people to unintentionally violate the DMCA, and too easy for copyright holders to enforce their will in ways that do not further the goals of copyright law.

179. Lipton, *supra* note 44, at 513.